NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

FINANCIAL TRANSACTION MECHANISMS FOR WORLD WIDE WEB APPLICATIONS

by

John R. Palumbo

March, 1996

Thesis Advisor: Hemant Bhargava
Associate Advisor: Rex Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE 28 March 1996	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE FINANCIAL TRANSACTION MECHANISMS FOR WORLD WIDE WEB APPLICATIONS	5. FUNDING NUMBERS
6. AUTHOR(S) John R. Palumbo	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.	
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The World Wide Web is the fastest growing application of the Internet. Its continual growth has provided a new electronic medium for commerce. One of the more exciting uses of the World Wide Web in commerce is the selling of information, instead of goods. A major obstacle that the World Wide Web in general and information sellers specifically faces for commercialization is secure means is conducting financial transactions. This thesis' objective is to develop a criteria for individuals to use in the evaluation of the different financial transaction mechanisms that are becoming available on the World Wide Web.

Two of the leading financial transaction mechanisms available today, First Virtual and Netbill, are analyzed in detail and compared on the basis of these criteria. This analysis is then applied to Decision Net. While First Virtual's is further along in the development process, Netbill promises to offer better features to the meet Decision Net's requirements.

14. SUBJECT TERMS Financial Transactions, World Wide Web, Internet, WWW, Decision Net			15. NUMBER OF PAGES 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

FINANCIAL TRANSACTION MECHANISMS FOR WORLD WIDE WEB APPLICATIONS

John R. Palumbo
Lieutenant , United States Navy
B.A., University of Oklahoma , 1989

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1996

Author: ______________________________
John R. Palumbo

Approved by: ______________________________
Hemant Bhargava, Thesis Advisor

____
Rex Buddenberg, Associate Advisor

____
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The World Wide Web is the fastest growing application of the Internet. Its continual growth has provided a new electronic medium for commerce. One of the more exciting uses of the World Wide Web in commerce is the selling of information, instead of goods. A major obstacle that the World Wide Web in general and information sellers specifically faces for commercialization is secure means is conducting financial transactions. This thesis' objective is to develop a criteria for individuals to use in the evaluation of the different financial transaction mechanisms that are becoming available on the World Wide Web.

Two of the leading financial transaction mechanisms available today, First Virtual and Netbill, are analyzed in detail and compared on the basis of these criteria. This analysis is then applied to Decision Net. While First Virtual's is further along in the development process, Netbill promises to offer better features to the meet Decision Net's requirements.

TABLE OF CONTENTS

I.. INTRODUCTION

A. INTRODUCTION

The Internet contains over 15,000 autonomous networks, with over 1.8 million hosts world wide (Brand, 1995). The World Wide Web (WWW) is a multimedia subset of the Internet that allows its users to observe hypertext, graphics, video, and audio data (Little, 1994). Although smaller than its parent, the WWW has an estimated two million viewers in the households and business of the world in 1994 (Little, 1994).

The future of electronic business on the Internet will most likely be the World Wide Web (WWW). The graphical nature of the WWW makes it easy to use for both computer literate and non literate users alike. This ease of use that is the cornerstone of the WWW, has led to its recent explosion of use (Brands, 1995). Many companies have already branched out into the WWW for not only reaching an ever increasing customer base, but also to maintain a steady forum for communications for their employees. A good example of this is the J.C. Penney Company.

In the past year J.C. Penney has established a WWW presence for customers to review the latest merchandise via the WWW's graphical interface, thus reaching a new market of potential customers. In addition, J.C. Penney has also established an *internal* web for access by their employees. This internal web is used for providing guidance and policy to all employees, computerizing some training material, and latest sales information. (Lessa, 1995)

This explosion and its expected rapid growth has brought many to the conclusion that the WWW may be used for commerce, not only for large corporations, but for almost any small

business with a computer, a modem, and a phone line. The key reasons why the WWW is ideally suited for commerce is its relatively low entry cost, low printing and distributions cost, multimedia applications, data automation, rapid customer feedback, and immediate information updates (Little, 1994) In anticipation of the commercial jump into the WWW, may companies have begun to offer different types of financial services (Dukach, 1992; Stien, 1994; Medvinsky, 1993; Wall Street Journal, 1994).

B. OBJECTIVES

The vast influx of financial transaction mechanisms (FTM) on the market may have left many users confused on which is best suited for their WWW applications. First, It is the goal of this thesis to establish a criteria for judging a FTM. Secondly it will use this criteria in a comparison of current FTMs. Third it will make a recommendation for the use of a FTM for Decision Net (DNet).

Decision Net is a WWW application that has the primary goal of providing decision support (DS) technology to users via the Internet. The primary architecture for DNet will have DS technology providers leaving their software packages on their own systems. This will keep both maintenance and publication costs low. DNet will then provide the necessary overhead to establish connection from the decision support platforms and the WWW. The customer will access the decision support technology via the DNet Yellow Pages. Although DNet is not currently a commercial venture, if it were to enter the commercial market place it would need a means to to recover cost associated with the creation of the necessary overhead, and provide financial restitution to the provider of a technology being accessed. (Bhargava, 1996)

Of all the FTMs currently being used on the WWW, two have been chosen based upon prominence in their realm, these are; First Virtual (FV), and Netbill.

C. METHODOLOGY

Becuase financial transactions on the WWW are still relatively new, most of the material can not be located in traditional bibliographical sources that are associated with normal research. The majority of research material was downloaded from various WWW sites across the globe. Due to the fluid nature of WWW resources, when possible the vital web pages were collected and placed into the Appendix.

In addition to the WWW sites, interviews were conducted when needed via electronic mail with individuals within the organizations.

II. PROBLEM DEFINITION

Four major difficulties face an individual in the selection of a FTM for their use. The first is the rather large number of FTMs on the market, while the second is the lack of standards and compatibility amongst the systems. The third is the type of company that is requesting services, and the fourth is the threats that are facing the users of an FTM. Each of these problems will effect the development of a criteria for the selection of a FTM, and will be briefly discussed.

A. NUMBER OF FINANCIAL TRANSACTION MECHANISM

At a quick glance, the number of FTMs available to the public are significant. They range from small entrepreneurs (First Bank, 1994) to large financial institutions (Siino, 1994). Each FTM follows a separate format for the exchange of funds between the customer and the supplier.

B. LACK OF STANDARDS

As with any emergent technology, one of the greatest problems that the FTM world faces is compatibility. Several standards bodies are looking into the security of electronic commerce for the WWW (Spyglass, 1994). However with no single dominant member of the market, many companies are pushing forward with their 'stove-pipe' systems with one hand while 'working' with the standards body with the other hand (Spyglass, 1994; Deephouse, 1995).

One of the more active bodies attempting to provide commerce standards for the WWW is the Internet Engineering Task Force (ITEF). However, as with most standards bodies, the work is slow due to the attempt to accommodate all points of views. Although not an official standards body, the World Wide Web Consortium (W3C), works with the ITEF to help bring

concepts and designs for open commerce protocols to the WWW in a swifter fashion. With that said, neither body has made in significant gains in developing an acceptable system. (W3C, 1995;IETF, 1995)

C. TYPES OF COMPANIES

The companies that would use a FTM vary in type and function. However, I have broken them into three basic categories based upon the type of goods or services offered. The three categories are:

- Direct sales: By far the largest type of company that can be found using a FTM. Direct sales will include the purchase of a wide range of goods that could include computer software, clothing, and art work.
- Information Sellers: There are two basic types of information sellers. They include those that actively seek unknown information and those that hold a repository of known data.
    - Agents and Brokers: The first type of information sellers are active hunters of on-line material. Whether a highly intelligent program (Agents) or a person (Broker) they provide the service of hunting for information, then charge funds based on the detail of the search and length of time spent on the search. Agents and brokers are relatively new, and may be a possible future for the internet and WWW.
    - Warehouses: The second type of information seller is Warehouser. These companies establish a vast store or databases that may contain intelecutal property of one form or another. This information can either be sold by the page or complete unit.
- Clubs or Organizations: The last of the categories provides payment for locations within the WWW notaccessible by the general public. This area is highlighted for the use of specific intrest groups.

Although each group has special needs, each has to have a base system that is suitable to their requirements. Throughout the development of the criteria, specific benefits and detriments to a company type will be highlighted.

D. THREATS

Although threats abound in a relatively new technology dependent system such as the Internet, the focus for this discussion will be on what I feel are the two primary threats. These are the hackers and the sniffers. (Tardif, 1995)

1. Hackers

Hackers are a group of individuals that have developed a great amount of computer skills. These skills allow them to actively 'break' into the computer files of the system that they are targeting (Fitzgerald, 1993). The first hackers were thought of in a 'romantic' air, breaking into systems for the challange. However as the skills began to proliferate, the break-ins become more and more hostile.(Tardif, 1995)

2. Sniffers

When the Internet was originally designed it was built to help facilitate the free flow of information, even at times of national crisis. To create an architecture that would aid this flow, many networks were connected in a vast number of configurations. If one route was lost, another would exist to take its place. (Tardif, 1995)

This openness is key to the sniffers ability to commit attacks. When a data packet journeys to its destination, it will travel through several networks (Fitzgerald, 1993). It is at these locations that a sniffer can intercept the data, read or alter its contents, and then send it on its way. If precautions are not taken, the person receiving the file may never know if the data has been compromised. (Tardif, 1995)

E. LOOKING FORWARD

The problems that face an FTM and therefore commerce on the WWW are quite broad in scope. It is hoped that the criteria detailed in the following chapter will provide the reader the necessary tools to determine if a particular FTM meets the goals that a user requires.

III. CRITERIA FOR FINANCIAL TRANSACTION MECHANISMS

The largest single problem facing full integration of the WWW into the business mainstream is the lack of a secure mechanism to conduct financial transactions (Gelormine, 1995). The factors facing a suitable financial transaction mechanism (FTM) are very wide in scope, and vary in importance in the opinion of the different developers. I will attempt to narrow the focus by concentrating on the unique problems involved with third party transaction systems. With that in mind it will be necessary to identify the players involved with the generic third party FTM. Four groups will be identified as having an interest in the FTM, these four are:

- Seller: The Seller is the individual or company that is offering information, goods, or services for sale.
- Buyer: The Buyer is the individual that is willing to financial compensate the Seller for delivery of information, goods or services.
- FTM Service Provider: The FTM Service Provider (or simply the Provider) provides the conduit for financial compensation. They establish the rules by which both the Seller and Buyer must agree in order to close a transaction.
- Threat: The Threat comes in the form of Hackers, Crackers, or Sniffers that, for their own reasons, have attempted to 'break' a Providers services.

Even by focusing on the generic third party FTM system, the number of variables are far too numerous to do a detailed analysis. To that end, criteria need to be developed to help evaluate individual FTMs and determine if they are suitable for use in either the government or private sector. I have chosen four areas that I feel the industry is focusing on. These areas will be the deciding factor in both the acceptance of the FTM, and its continued success. The four focus areas are security concerns, traceability or lack of it, the system's ease of use, and transferability between customers. The four areas are not exclusive sets, and will often overlap amongst themselves. When this occurs, every effort will be made to establish this link.

A. SECURITY

The foremost of area of concern is that of security. News reports constantly emphasis the facts of Hackers/Crackers that have broken into the phone systems and banks at an alarming rate. (Carter, 1995) With financial transactions starting to go across the WWW, it will not take long for these cyber-criminals to start developing tools to steal (hacker) or intercept (sniffer) FTM signals. This threat would be detrimental to not only the merchant that would lose revenue, but also the customer who might lose credit card numbers, or the FTM provider that would lose the good will of its clients. It is for these reasons that security of an FTM is the most vital of focus areas.

Because security can cover such a wide range of topics, I have broken it into two distinct functions. Although they overlap in some areas, I feel that they perform separate goals and should be addressed separately. The functions consist of integrity and reliability.

1. Integrity

Integrity of an FTM is a pivotal concern to all members involved in a financial transaction. Although a rather broad term, integrity of a system could be exhibited by the following. (Janson,1995)

- Debit authorization forms (checks) must be electronically signed by the purchaser prior to the release of funds to the seller.
- Each signed check must be unique, so that the seller (or sniffer) can not resubmit the payment.
- Receipt of goods or services should be available for the purchaser.
- A guarantee of payment from the buyer to the seller **prior** to the transfer of goods or services.
- The ability for the buyer to view the goods **prior** to the transfer of funds. (Easy for viewing goods via pictures, difficult if attempting to view information.)

Integrity of a system can be difficult to engineer. For example, the last two criteria appear to run contrary to each other. The provider needs to determine whether they are serving the seller or the buyer. One that is serving the buyer will have a emphasis towards viewing a product prior to payment, while a provider favoring a seller will ensure that payment is received prior to the release of the product. In addition, the type of seller will determine the integrity. For example, an Information Seller would be able to show a prospective customer the information first hand. However, it would be difficult to have Direct Sales let a Buyer hold the object being purchased.

An FTM that has strong integrity security would exhibit all of the above in varying degrees. Most current FTMs on the market offer only a few of the four criteria, making integrity one of the driving concern in the FTM selection. Figure 1 gives the evaluation scale to be used for integrity.

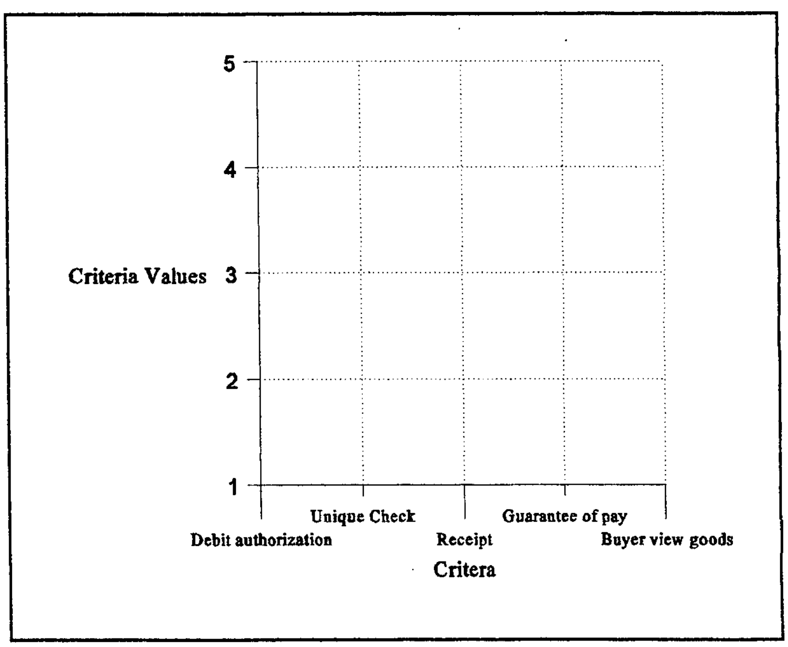

Figure 1 Criteria for Security: Integrity

2. Reliability

The second security issue deals with reliability. Although it may have the appearance of being less important then integrity, reliability still plays a major role. Issues that need to be addressed when looking at the reliability of a FTM system should include the following.(Janson,1995)

- Due to the global presence of the WWW, transactions must be able to be handled 24 hours a day, seven days a week.
- Payments must be completed. No payment should be partially completed.
- The FTM system should have back-up capability to allow for system down time.

An FTM offered on the market should be able to answer the concerns of a either the buyer or seller as the reliability of the hardware that the FTM is running. In addition the FTM should provide reliability statistics for both hardware and software downtime to prospective customers and current users on request. Figure 2 shows the criteria scale for reliability.

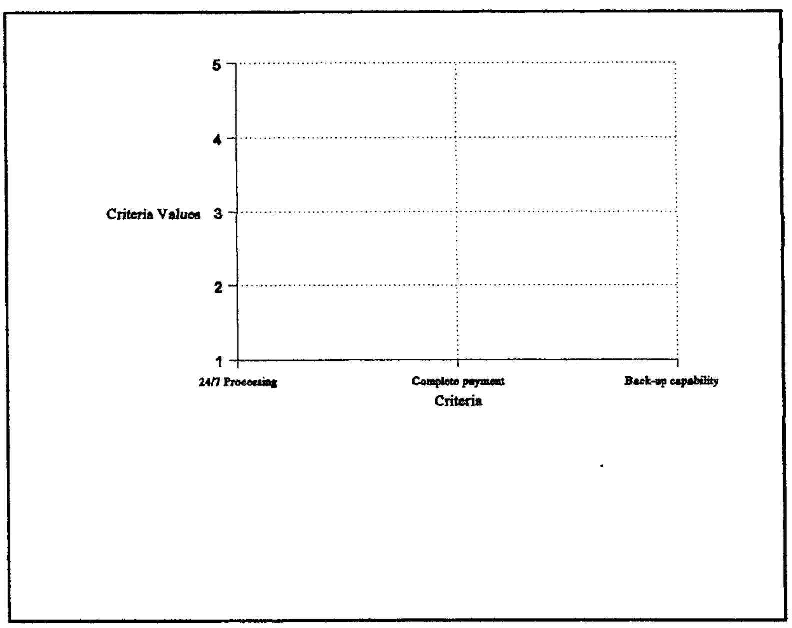

Figure 2 Criteria for Security: Reliability

B. TRACEABILITY

Although security is vital to the establishment of a truly successful FTM, it can not be the only criteria. In the civilian world the second highest priority is most likely traceability. The traceability concern has its roots in the privacy of individuals to interact without interference from external scrutiny. The key violation of traceability comes from the inevitable "paper trail" that follows any transactions. In most FTMs this paper trail is located in a centralized database (Cox, 1994). This database, if obtained, could be used for activities ranging from massive direct marketing campaigns, focus for criminal activity, or illegal search of information by law enforcement authorities.

In addition, not only should the paper trail be of concern, but also the content of the purchase and for what amount. There is a fine line between providing sound privacy for the users of an FTM system, and accidentally breaking tax laws. Although the Internet does not respect the boundaries of states or nations, its users will be expected to comply with all the laws in their respective local areas. The tax codes vary from state to state, but each requires payment of a sales tax on some goods. In addition, transactions in excess of $10,000 are subject to scrutiny by the IRS. (IRS, 1996)

To help identify if a FTM is providing reasonable privacy, but not breaking any existing laws, the following list of criteria could be used.

- Secure servers, using the highest technology of fire wall protection.
- Proper tax filling procedures, or instructions on purchases of excessive size.
- Alternative individual identification formats.
- Multi-level security for customer database files.

It should be obvious that the transferability issue and the security (particularly integrity) are closely related in many ways. But it should be noted that the Buyer should understand what level of privacy he can expect with a system. If it is an issue for the user, than they should look closely to the FTMs approach. Figure 3 shows the criteria scale for transferability.

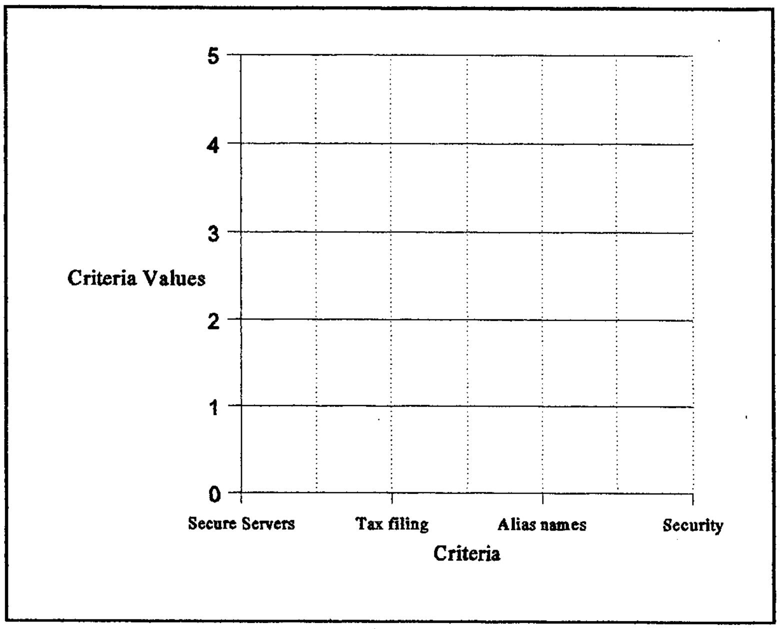

Figure 3 Criteria for Traceability

C. EASE OF USE

The third primary criteria for the selection of a FTM is the systems ease of use. Since the home computer market has opened, the number of users has grown significantly each year. The primary reason for this continued growth is the ever increasing ease of use of the systems. In the PC realm, the first systems ran using DOS operating system. It was difficult to master, configure, and operate. This led to only a handful of users. When Microsoft introduced its 1.0 version of the Windows software, an interface that made running the computer much easier, in 1983 the PC industry had sold approximately 500,000 units. (Polsson, 1995)

By the time Microsoft released its 3.0 version of Windows in May of 1990, the number of single computer users had jumped to 9.8 million. Of this number over 8 million were based on the Intel family of microprocessors. More startling perhaps is that another 1.3 million of this number were Apple's Macintosh family of computers, which contains another popular user interface. (Polsson, 1995)

In 1995 Microsoft delivered the much anticipated Windows '95 operating system. The new system made it not only easy to work with computer, but made hardware instillation a much simpler task. The Windows '95 release broke all the commercial off the shelf software sales records, once again proving that more users will flock to a easier to use. (Polsson, 1995)

How does this relate to FTM? Simply that more users will have access to the WWW and they will wish to conduct financial business over the web. This growing number will be less computer literate then their predecessors. These users will not want to install new hardware designed for encryption, nor will they want to learn all of the steps in running a complicated public key encryption system. They will want to use a system that allows them to simply click the 'go' icon, and let the system do the work for them. This feature is called "click and go". It is with this in mind that the designers must make all the security measures invisible to the user. (Brands, 1995)

Below is a list of items that should be looked at in detail when investigating FTM systems.

- Configuration requirement simple to follow.
- Availability of technical support.
- "Click and Go" approach.
- Number of steps to execute payment.

The needs for ease of use and security may seem to be in opposite to each other, and in many ways they are. However, the FTM needs to be able to adjust to the growing demands of the market. People will want security, they just will not want to work for it. Figure 4 shows the criteria scale for ease of use.

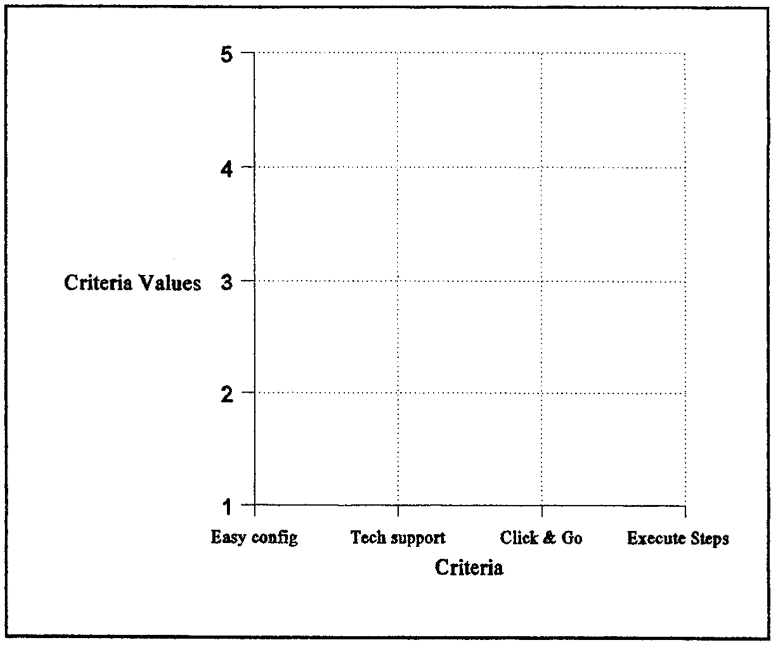

Figure 4 Criteria for Ease of Use

D. TRANSFERABILITY

The last of the key areas is transferability. In a open currency system, such as the US dollar, money may be exchanged between two private parties with little effort. In a open FTM one customer would be able to transfer money to another customer, in addition to a business. Although this area will not be of high interest to DOD, the civilian market may find it a highly desirable item. Although technically feasible, it will be difficult for most FTM system to establish such a system that will be both financially rewarding for themselves, and acceptable to the users.

Most FTMs make their money from 'taxing' the total amount of the purchase. For example, if a Customer purchased a chapter from a book for two dollars, he would send his voucher/check to the FTM. The FTM would then keep a portion of the two dollars, ranging from, say, two to ten cents, and forward the remainder to the Sellers account. When two Customers decide to exchange funds, neither Customer would be willing to forgo the FTM's percentage cut. How the FTM deals with this procedure, or if it is allowed, is last of the key areas.

The World Wide Web has quickly become an instant arena for advertising, it is not hard to imagine true commerce being to far behind. The first major obstacle is the acceptance of a Financial Transaction Mechanism to be used both by the seller of goods and services and the buyer. The FTM chosen will limit the buyer to a set of sellers do to the differences in approaches by the FTMs.

IV. SYSTEM REVIEWS

A. FIRST VIRTUAL

1. History

First Virtual (FV) founding members reads like a who's who of the business and Internet worlds. Initially incorporated in March of 1994, FV is a privately owned company. The founders are Lee Stein, a prominent figure in the San Diego business community, Tawfiq Khoury, a land developer in southern California and Arizona, Nathaniel Borenstein, chief author of the Internet standard format for interoperable multimedia data (MIME), Marshall Rose, an area director for Network Management in the Internet Engineering Task Force, and Einar Stefferud, founder of Network Management Associates, and Internet pioneer since 1975. These individuals along with their strategic partner, Electronic Data Systems, a credit card and automated clearinghouse transaction company, have worked together to create a system that does not create 'cyber money' but uses current standards to establish secure credit card transactions over the Internet. (FV Background, 1995)

2. Procedures

a. Account Acquisition

To establish an account as a customer, it is as simple as point and click. Once the user is at the FV home page (http://www.fv.com), they click on the new account button. The user is instructed to fill out information presented on the form, along with a password of the users choice. No credit card information is passed over the Internet. When FV receives your request for an account, you are sent an E-mail that contains follow on instructions for purchasing the account, including an 800 number that must be called. When the user calls the 800 number

they are greeted by an electronic voice mail system that helps them finish the transaction. It is only during this telephone conversation that any credit card information is transferred. Although the phone system is technically no less secure then the Internet, it does provide the user with the sense of security. With in a few hours the member is sent a new account pass word via E-mail. The new password consists of the users original, plus a specific prefix that is provided by the company. (FV General, 1995)

b. Sample Transaction

Transactions on FV are conducted using a simple E-mail-based protocol. To initiate a purchase the Customer simply "clicks" the purchase button located on the page containing the information that they wish to purchase. This button initiates a E-mail form that allows the Customer to enter his or her password. When the E-mail is sent, the Seller may allow the Customer to have access to the information requested.

When a FV receives the requests for fund transfer, it will automatically send E-mail to the customer. The E-mail is structured to permit automated handling by mail software that understands the protocols used by FV, but also to be completely usable with most ordinary mail software. When the Customer receives the FV mail, they simply have to use the mail reader's "reply" command, and send a reply using a single word of either "yes", "no", or "fraud". The receipt of a "yes" answer with an appropriate transaction code in the Subject line and appropriate source headers in the E-mail constitutes the buyer's authorization to First Virtual to effect a fund transfer. A reply of "no" or "fraud" would not allow the transfer of funds, with the "fraud" initiating necessary procedures to determine the source. For this mechanism to work, the mail reader's reply command should copy the contents of the Subject field into the reply,

because it contains a unique identifier for each specific authorization request. Customers must also have instant access to their respective E-mail accounts at all times.(FV Cashflow, 1995)

Real funds begin to flow only after the authorization is received and the transaction is passed to what FV calls the "below-the-line" (BTL) systems. The BTL system contains a database that correlates all FV account identifier with a Customer's credit card information, and the Sellers checking account information. (FV Cashflow, 1995)

When a fund transfer request is received by the BTL system, it is added to the list of charges awaiting settlement by the Customer, but not yet paid. If the total amount of charges on the Customer's settlement list exceeds $10, the system will post a charge for the appropriate amount to the Customer's credit card, using the credit card network to pre-authorize the transaction. Otherwise, the charge accumulates until the $10 threshold is exceeded or the oldest transaction has been pending for more than 10 days. When a charge is posted to Customer's credit card the on-line portion of FV is notified, and an E-mail notification is sent to the paying party. (FV Cashflow, 1995)

After the funds have been received from the Customer's credit card company, FV deducts the transaction fees. The fees are discussed in the section below. The remaining amount is transferred to the seller's checking account by the BTL system. When this is accomplished, the On-line system will notify the Seller that a transaction has been posted to their account. (FV Selling, 1995)

3. Cost

a. Customer

The customer pays an initial fee of two US dollars for registering the account. If the customer wishes to change account data, like changing to a new credit card, the customer will be charged an additional two US dollars. Any fees after this are directed to the supplier. (FV Buying, 1995)

b. Supplier

The charges that a supplier pays is dependent on where the information being sold is located. All suppliers pay an initial $10 registration fee. If the supplier is not using FV's Infohaus, they pay 29 cents for each purchase, plus two percent of the total sale to FV. When funds are transferred to Supplier, an additional charge of one dollar is collected for processing fees. (FV Selling, 1995)

Those that use the Infohaus are also charged the same 29 cents per sale, but they must also pay an additional eight percent of the total sale value to FV. In addition FV charges the users of the Infohaus $1.50 per megabyte of storage per month. The totals charged by FV approach 2% for those Sellers that maintain their own location, and 10% for those using the Infohaus. (FV Infohaus, 1995)

3. FTM

FV would not provide me an estimate of how much it cost to execute a typical transaction, however it is reasonable to assume that FV pays the standard transaction cost that all financial institutions pay when dealing with an electronic transaction clearinghouse.

A. NETBILL

1. History

Netbill began as a research project in early 1991 at Carnegie Mellon University's (CMU) Information Networking Institute (INI). The principle researchers have been Marvin Sirbu, a professor of engineering and public policy and industrial administration, and Doug Tygar, an associate professor of computer science, both at CMU. The initial goal of Netbill was to provide a means of making transactions for small amounts of information, and keeping the processing fees associated with this transaction in the range of one to ten cents. (VISA/CMU, 1995)

In February 1995, CMU and Visa International announced that they have formed a partnership to develop and conduct trials of the Netbill system (VISA/CMU, 1995). These trials are expected to occur by mid 1996, with a full production version ready for use on the WWW by fourth quarter 1996. (Deephouse, 1996) Visa has viewed this project as one portion of its plan of supporting the needs of its members in the electronic commerce market.(VISA/CMU, 1995) Netbill is in the process of negotiating with companies such as Netscape and Intuit (the makers of Quicken) to bundle Netbill with their software products. (Deephouse, 1996)

2. Procedures

a. Account Acquisition

Although Netbill has not started to accept applicants for customers or sellers, it is believed that all of the registration will occur on line, via the use of WWW forms. These forms would be linked to the Netbill software, and provide the necessary security for private information.

b. Sample Transaction

The Netbill transaction starts when the Customer requests a price quote from the Seller. The Customer requests a price quote by simply clicking on a displayed article reference. The Customer's client application then indicates to the *checkbook library* (Netbill's Customer accounts database server) that it would like a price quote from a particular Seller for a specified product. The *checkbook library* sends an authenticated request for a quote to the *till library* (Netbill's Sellers accounts database server) which forwards it to the merchant's application. (Netbill, 1995)

The Seller must then determine the price for the authenticated user. He returns the digitally signed price quote through the *till library*, to the *checkbook library*, and on to the Customer's application. The Customer must then make a purchase decision. Assuming the Customer accepts the price quote. The *checkbook library* then sends a digitally signed purchase request to the Seller's *till library*. The *till library* then requests the information goods from the merchant's application and sends them to the customer's *checkbook library*, encrypted in a one-time key, and computes a cryptographic checksum on the encrypted message. (Netbill, 1995)

As the *checkbook library* receives the bits, it writes them to stable storage. When the transfer is complete, the *checkbook library* computes its own cryptographic checksum on the encrypted goods and returns to the *till library* a digitally signed message specifying the product identifier, the accepted price, the cryptographic checksum, and a timeout stamp. This collection of data is called the electronic payment order (EPO) by Netbill. (Netbill, 1995)

Upon receipt of the EPO, the *till library* checks its checksum against the one computed by the *checkbook library*. If they do not match, then the goods will either be retransmitted, or the transaction will be aborted. Netbill hopes to provide high assurance that the encrypted goods were received without error. If checksums match, the merchant's application creates a digitally signed invoice consisting of price quote, checksum, and the decryption key for the goods. The application sends both the EPO and the invoice to the Netbill server. (Netbill, 1995)

If the Customer has the necessary funds or credit, the Netbill server will debit the Customer's account and credits the Seller's account, log the transaction, and save a copy of the decryption key. The Netbill server then returns to the Seller a digitally signed message containing an approval. (Netbill, 1995)

3. Cost

a. Customer

The cost to the customer will most likely be negligible. This is dependent upon the strategy used by Netbill. Customer based software may be available free of charge via the WWW for personal use. Professional or commercial versions may be introduced at a cost as the project develops. Netbill will also try to attempt to market themselves by 'bundling' the Netbill software to other popular software titles, such as Netscape and Quicken. (Deephouse, 1996)

b. Supplier

The supplier will be charged a very low flat fee of approximately $.02 per transaction. In addition the seller will be responsible to pay a fee of 2%-5% of the total sale for the processing of a transaction. Netbill currently has no plans to develop an electronic market place, this means that each user must have access to their own resources in order to use the system. (Deephouse, 1996)

c. FTM

Netbill is expecting to pay the same electronic clearinghouse fees as all financial institutions. (Deephouse, 1995)

C. REMARKS

The methodologies of the two systems reviewed in this chapter are very different in their approach. In the next chapter we will look at each FTM using the criteria developed in Chapter III, and rate them. During this rating, we will focus on the FTM usage as applicable to a seller of information, particularly to the needs of Decision Net.

V. SYSTEM ANALYSIS

In this chapter, I will use the criteria developed in Chapter III on the FTM systems discussed in Chapter IV. Our primary focus will be the FTM's use in the selling of information, as it would apply to Decision Net. Scoring for each criteria will be based upon the documentation provided by the providers of the FTM services, actual use of the system when available, and E-mail interviews with the providers.

A. FIRST VIRTUAL

1. Security

First Virtual's policy towards security measures has always been to keep confidential information about customers off the Internet. To this end they have developed a protocol that uses e-mail, passwords, and usage notification on the open network, and keeps all critical financial records off line. (FV General, 1995)

a. Integrity

Overall FV does a good job of providing integrity to their customer base, with an average score of 3.4. The Figure 5 below shows FV's ratings in each criteria.

Debit authorization and the need for unique checks is conducted, not through electronic signature, but through response to e-mail messages received by the Customer from FV. After a purchase is made, FV sends an e-mail to the Customer, asking if they did, in fact, make said purchase. If the Customer does not respond to the purchase notification FV does not forward any funds to the account of the seller, and closes the Customers account to determine who used the FV account. (FV Buying, 1995)

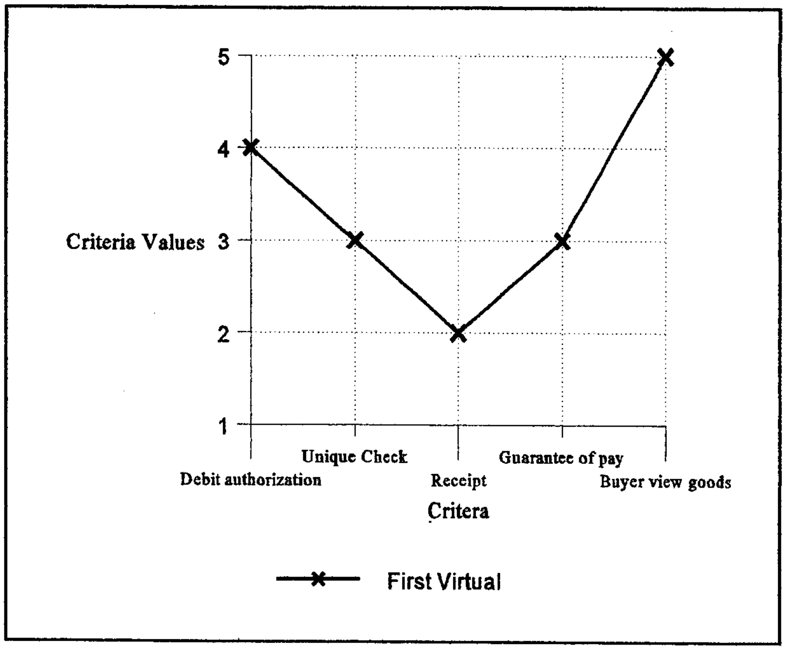

Figure 5. First Virtual Security: Integrity Scores

FV received poor marks for Receipt of goods because it offers no formalized receipt system. They consider the copy of your notification notice to be your receipt. However, no summary receipt is sent to the customer.

Part of FV is based upon trust of the customer. FV encourages Sellers to transmit purchased information, prior to the transfer of funds. FV feels that this model will help stimulate the use of the protocol, and minimize the loss to Sellers. The protocol gives the Customer the ability to pay or not to pay (based upon the notification message discussed above), this gives them ample time to review the information before funds are transferred. FV feels that they can police their users, and identify those that are abusing the protocol. (FV Security, 1995;FV Selling, 1995)

b. Reliability

FV scored an average of 4.3 for reliability. Figure 6 below shows how FV broke out in the criteria. Hardware and technical knowledge used by FV provide more than the

necessary skills and equipment to run both a continual (24/7) operation, and provide significant back-up capabilities for both on-line and off-line systems. The ability for FV to complete payments could be a potential problem. The interaction between the on-line and off-line systems is an unknown (for security reasons). Due to this and FV policy of purchase notification, FV's ability to complete payments in times of hardware problems is unknown.

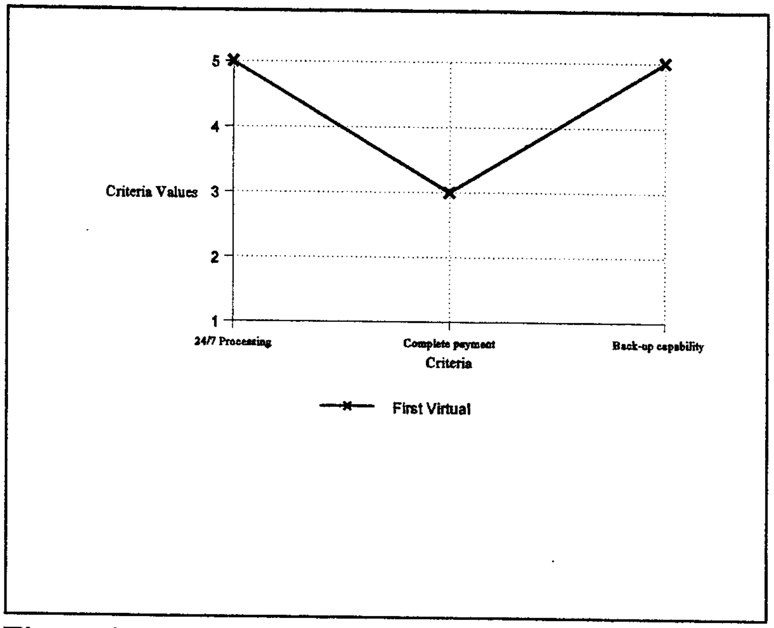

Figure 6. First Virtual Scores for Security: Reliability

2. Traceability

First Virtual scored an average of 4.0 for its traceability issues. The detail listing of scores is illustrated in Figure 7 below.

FV stated that they have are running one of the best fire-wall protection systems available, but would not elaborate in any greater detail. The fire-wall is used to screen incoming request, an additional firewall is used in the interface between the on-line and off-line systems. FV claims to honor the tax codes, but was quick to point out that it is the users (Customer or

Supplier) responsibility to ensure that proper tax codes are followed for any transactions that take place. (FV Security, 1995)

The Customer may use an alias for the purchase of on-line material, as long as the alias matches the name on the record at FV. Since FV holds the credit card numbers or bank accounts of each of its users, the use of an alias may only be effective with point of sale. This to may be a jeopardy based upon the seller's servers ability to record hits. (FV Buyer, 1995)

Multi-level security is difficult to manage, and FV may only provide a limited amount. (FV Security, 1995) Any data that is associated with an account, name, alias, purchases made, and account numbers would be available to any entry. It is believed that even a lawful entry, under a law enforcement warrant, would provide all data, even data that is not under warrant. (FV Security, 1995)

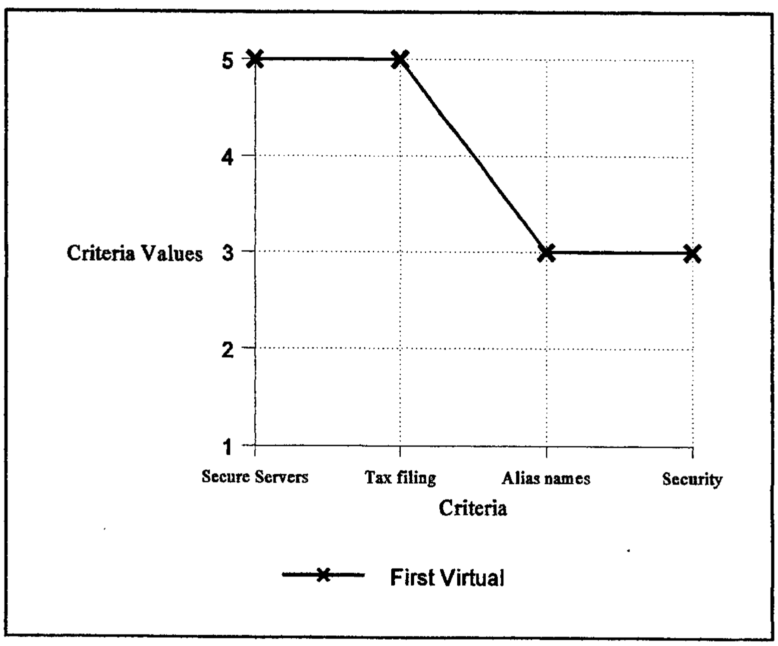

Figure 7. First Virtual Scores for Traceability

3. Ease of Use

FV's average score for Ease of Use is 4.0. The detailed scores for FV can be seen in Figure 8 below. FV's use of standard mail tools, and lack of user software, provide a quick and easy system for establishing service. FV tech support is readily available via the Internet (E-mail) or by telephone. FV also will provide the necessary form tools to help establish the FV transactions on Sellers Home Pages.

The only difficulty that I had with FV was the number of messages necessary to complete a transaction. A normal transaction will have three messages that are generated and sent to the Customer. With out proper mail organization, this could be cumbersome.

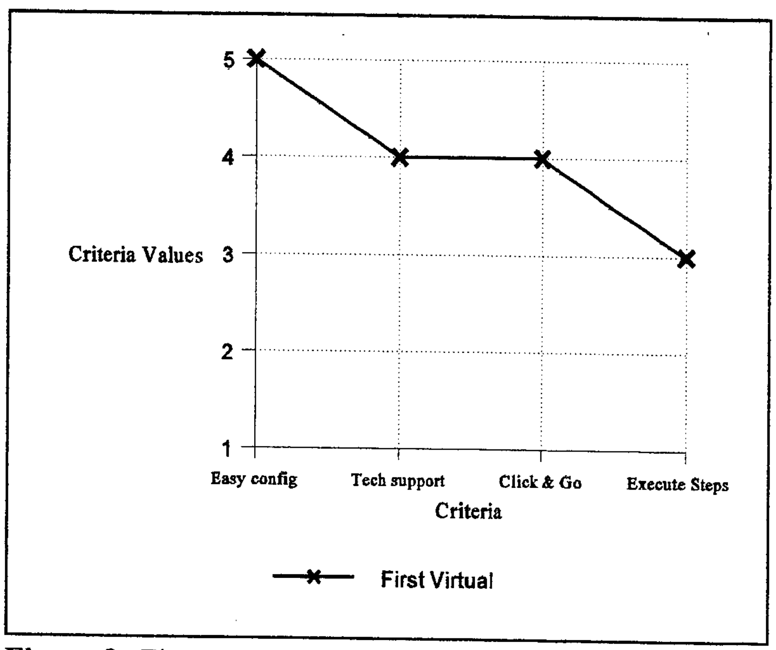

Figure 8. First Virtual Scores for Ease of Use

4. Transferability

First Virtual provides no capability for the transfer of funds between two customers. They only solution to this would be for one of the customers to be a Seller. However the transfer would also be subject to all of the charges that a normal transaction would acquire. This would be unacceptable undermost circumstances, therefore, FV's transferability score is 0.

B. NETBILL

1. Security

Netbill's basic strategy is the use of encryption at the three points of a transaction, that being the Customer, Seller, and Netbill. This may be difficult to engineer, but it appears that Netbill will be successful in completing the task.

a. Integrity

Netbill's average score for integrity is 3.8. Netbill's protocol is predicated on establishing electronic signatures with the combination of public key encryption to establish the necessary security needed for an FTM. The scores for debit authorization and check uniqueness is based on the Netbill protocol.

The ability for the Customer to view goods prior to purchase is a little unclear, and could be determined by the Seller, and be out of the control of Netbill. The guarantee of payment is rated at a four based on the need for Netbill to interconnect with the credit card network to ensure that the Customer has proper funds or credit available for the transaction.

As with FV, Netbill fails to establish a system for the delivery of a receipt of goods. This could be a difficult situation for the Customer who may need the receipt for tax purposes.

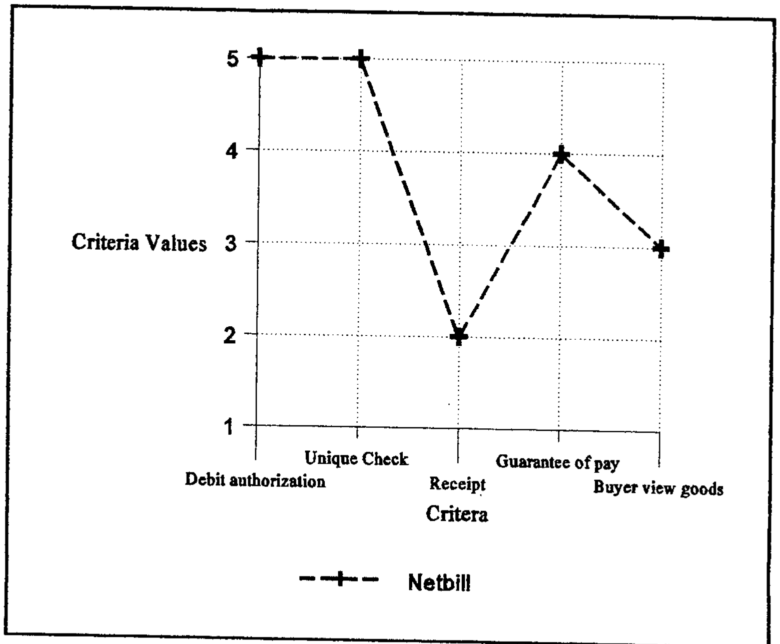

Figure 9. Netbill Scores for Security: Integrity

b. Reliability

Netbill scored very well in the reliability criteria, with an average score of 5.0, details can be seen in Figure 10. Netbill currently is running on proper equipment to continue both 24/7 processing and maintain the necessary back up capabilities that is critical to an FTM. In addition, one of the key points in the Netbill protocol is the atomic nature of payments (Netbill, 1995). This means that if a transaction can not be completed, it will not be undertaken. This will eliminate 'lost' transactions, and provide stability in the process.

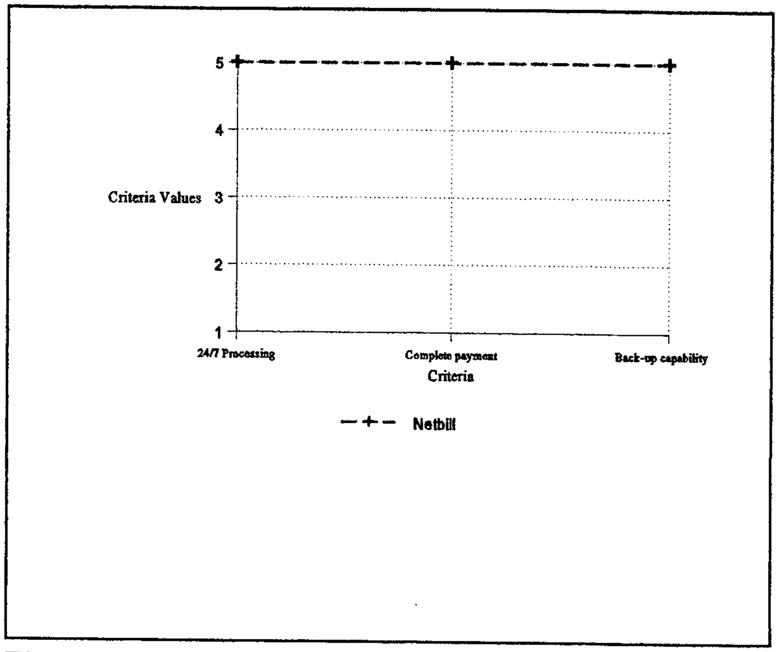

Figure 10. Netbill Scores for Security: Reliability

2. Traceability

Netbill's average score for traceability is 4.3, and Figure 11 below shows the scores achieved in criteria. It appears that the Netbill servers are secure and should not be a problem in the future. Also, with the assistance of Visa International, Netbill should not have any problems proper tax reporting. Netbill's Multi-level security is achieved by the use and maintenance of the encryption session key used for a transaction. If warranted law enforcement needs access to the data base, they would only be able to see data pertaining to the session that they have the right to view. The others would be encrypted under their particular session key.

As with FV, Netbill's ability to allow the Customer to use an Alias is limited due to the use of the Customer's credit card account for closing a transaction. However, some form of pseudonym may be maintained between the Customer and the Seller.

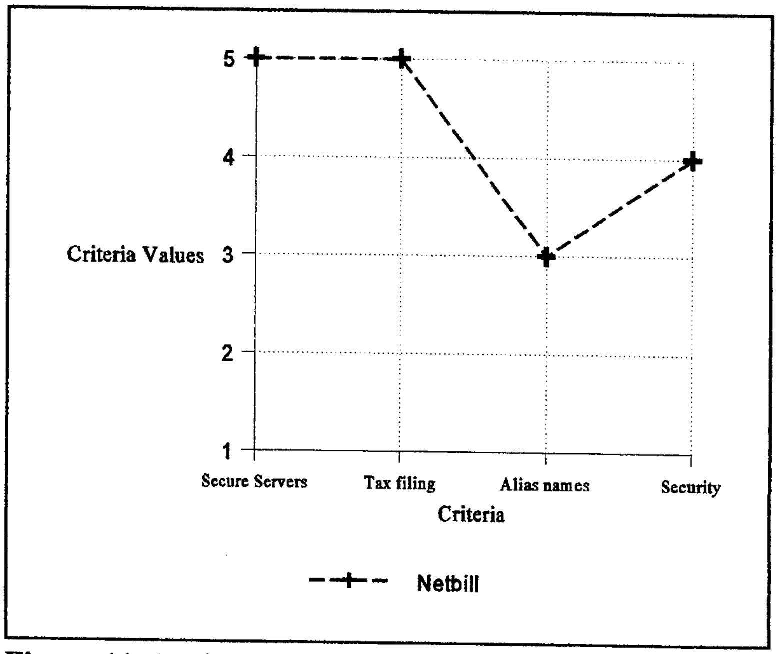

Figure 11. Netbill Scores for Traceability

3. Ease of Use

The average score for Netbill's ease of use criteria is 3.8, with Figure 12 providing the detailed scores. Because Netbill has not been released and has not even started trial runs, I was unable to 'play' with the system and get the feel for its ease of use. For that reason, most of this section is based upon 'impressions' received about the systems appearance, and not from hands-on use.

The first appearance of Netbill will be software that will need to be installed by the user. Not only will it need to be installed, but it will also need to be configured for the users browser, and Internet mail service. This is the reason for the low score in easy configuration. If Netbill provides a wizard tool that does most or all of the work for the user, then this score could change. However, once Netbill is properly installed, the purchase of information will become

simple point and click operation for simple purchases, with little to no follow on work by the customer.

Once Netbill becomes on-line, they have developed plans for available technical support via both the Internet, and standard telephone support.

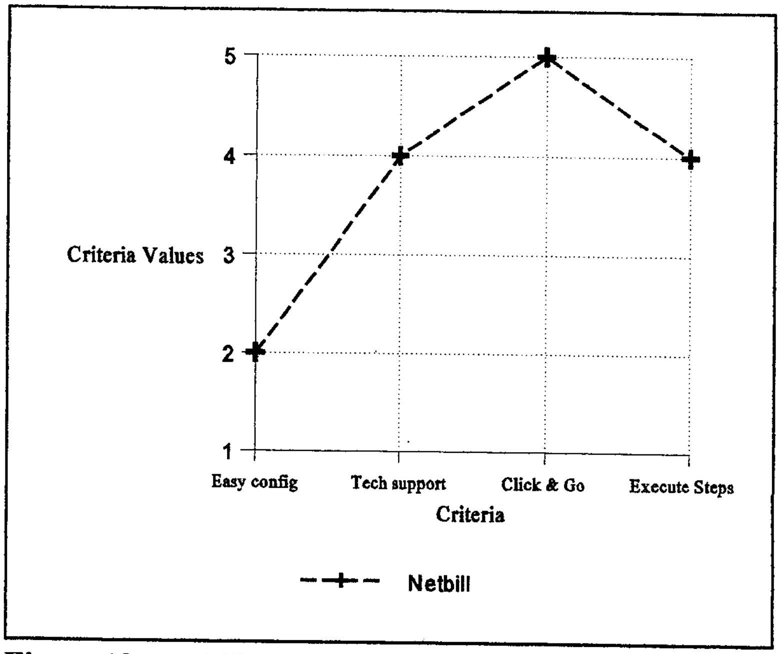

Figure 12. Netbill Scores for Ease of Use

4. Transferability

As with First Virtual, Netbill provides no capability for the transfer of funds between two customers. For this reason, Netbill's transferability score is 0.

C. COMPARISON

In this section I will compare First Virtual and Netbill. By comparing the two FTMs I hope to identify and emphasize the strengths and weakness of each.

1. Security

a. Integrity

The approaches that Netbill and FV took towards providing the necessary integrity of a transaction messages are quite different. I feel that Netbill's approach though provides a far superior solution to that proposed by FV. The primary reason for this is Netbill's use electronic signatures in their protocol. The ability to mimic or duplicate a customers or sellers electronic signature is far greater than the necessary skills need to defeat a FV message. Figure 13 provides comparison scores for the two companies.

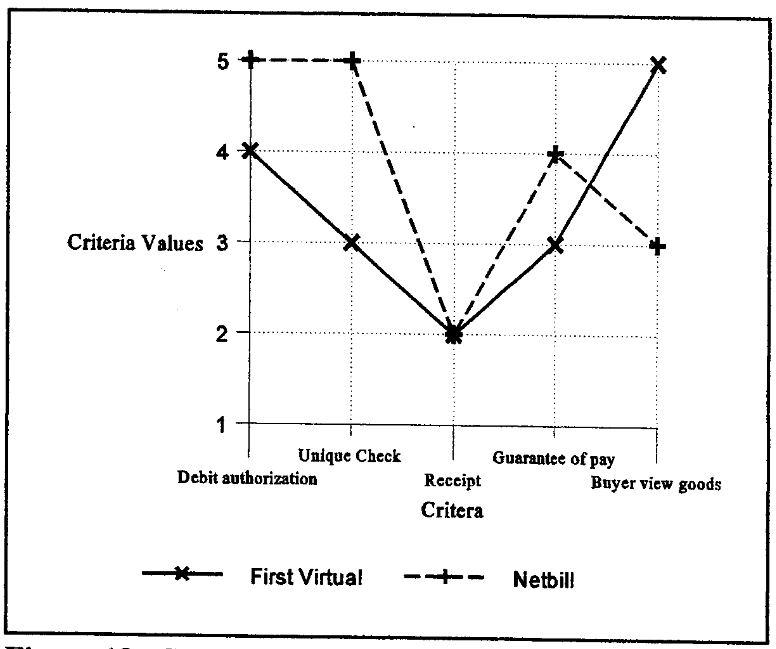

Figure 13. Comparison Scores for Security: Integrity

b. Reliability

Netbill's protocol once again provides a superior procedure than FV. Netbill's insistence that a transaction be atomic, is one of the keys of the system. FV failed to mention any protection for 'lost' transactions, making it a target area for possible hacker activity. Figure 14 below shows the comparison of scores.

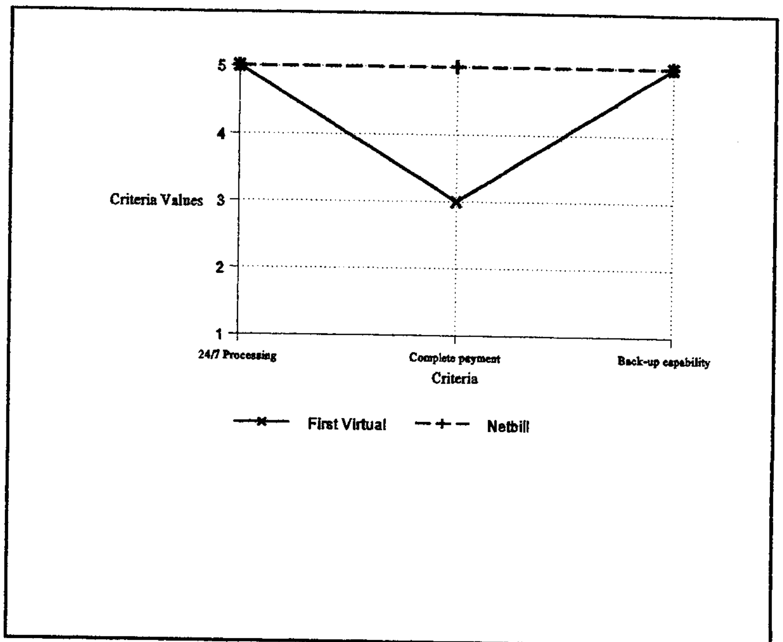

Figure 14. Comparison Scores for Security: Reliability

2. Traceability

The two systems scored very closely in the traceability criteria. The only significant score came in the multi-level security criteria. I scored Netbill higher in the category for their use and maintenance of session key cryptography. Each transaction is stored encrypted with the key that was used in the transaction. This allows for the privacy of all the other data that may be stored in the same database. Figure 15 shows the scores.

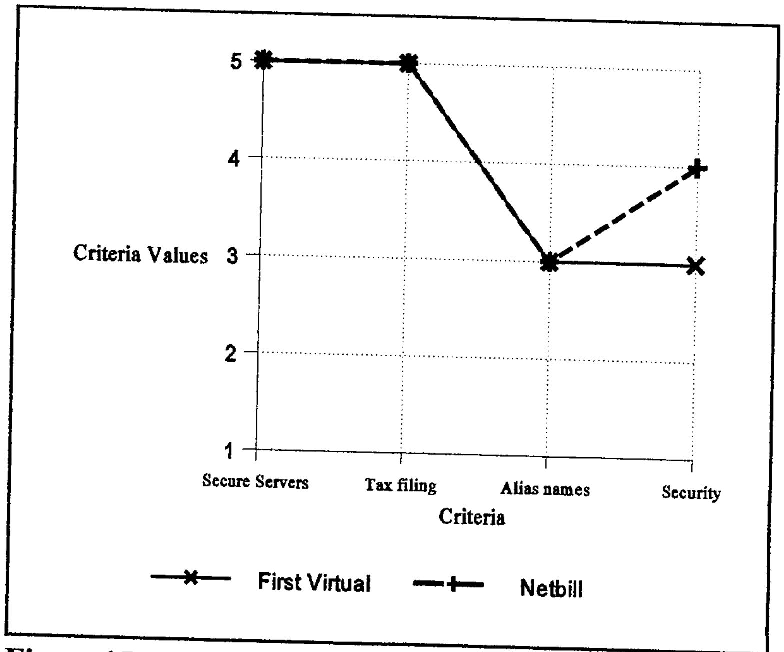

Figure 15. Comparison Scores for Traceability

3. Ease of Use

The Ease of Use criteria was the only one in which FV scored superior to Netbill. There are two distinct reasons for this. First, FV was designed to be simple, and it is, especially for the customer. However this simplicity has created some weakness in the system compared to Netbill. The second reason is my inability to actually use Netbill. In my opinion, Netbill's most serious problem will not be its security, buts its ease of use. What may be a significant benefit for Netbill is if they are successful in getting their product shrink-wrapped with either Netscape or Quicken. The comparison scores are shown in Figure 16 below.

4. Transferability

Neither Netbill nor FV had the capability to transfer funds between to customers. This is primarily due to the need of the FTMs to recoup the cost of the transaction, and the framework that each was designed upon.

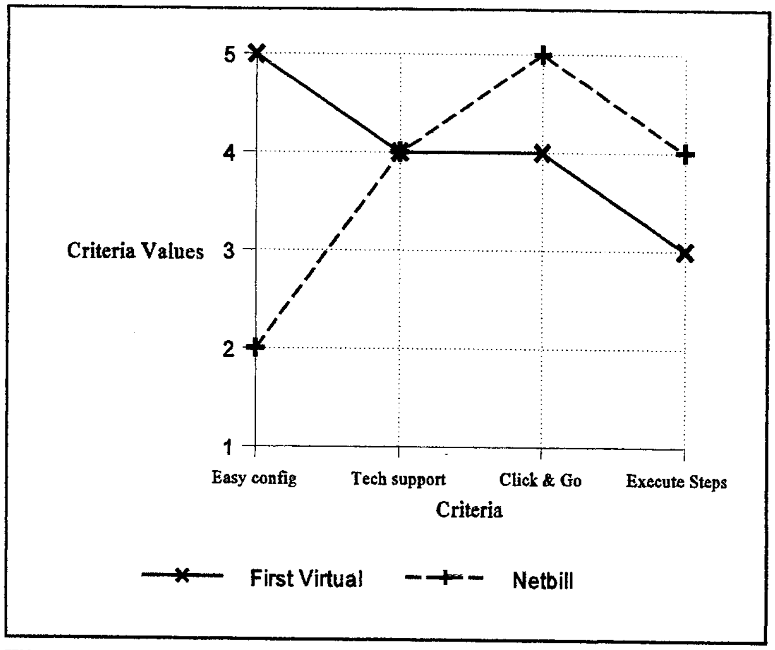

Figure 16. Comparison Scores for Ease of Use

D. REVIEW

Netbill appears to be a superior Financial Transaction System then First Virtual. The primary reason for this is Netbill's superior performance in the areas of 'Integrity', 'Reliability', and 'Traceability'. Netbill's single major weakness at this time is its 'Ease of Use'. Until Netbill is released on the market, a true evaluation of its usability will remain unknown.

VI. CONCLUSION

A. RECOMMENDATIONS

After reviewing the FTMs using the developed criteria, and my understanding of how Decision Net is to operate, the best recommendation that I can give is to wait. Although FV has gained a popular following on the WWW, I feel that Netbill will be a much better system. In addition changes in the FTM market that should take place within the next year or two will have a dramatic effect on the best option for establishing a charge back system for Decision Net's use.

B. SUMMATION

If all current predictions remain true, the World Wide Web will continue to grow in size and popularity for several years. This continued growth will inevitably lead to a large increase in the WWW's use for commercial purposes. The growth of client push/server pull capability will foster the ability of advertisers to bring commercialization to individuals, whether they wish it to or not.

This continued growth will see the use of some form of financial transaction. I hope that I have been able to create a starting point for people to investigate the FTM's as they become available on the market. However, due to the rapidly changing face of the WWW, the information detailed in this thesis is already dated.

As an additional note, companies may start to use more than one FTM for the selling of goods or services. The primary hope of the companies using this tactic would be to gain a larger market share by giving more payment options. But before going down this path the seller must

market share by giving more payment options. But before going down this path the seller must determine if the additional overhead cost of supporting separate payment mechanisms is worth the additional revenue that it might generate.

C. FURTHER RESEARCH OPPORTUNITIES

At first glance, their are several branches that lead itself to further research. I have listed a few ideas below.

- Electronic Servmart: Establish a protocol that would allow the use of the WWW in the creation of an electronic servmart. This entity could increase efficiency at a servmart by allowing the customer to browse the store and make purchases without every leaving their command. Once an order has been placed, it could be processed and waiting for pickup by a commands duty driver.
- Protocol Analysis: Conduct a detailed analysis of the Visa/Master Card proposal and or protocol. Establish its ability to be adapted for use by the Department of Defense or the Department of the Navy.
- Research Funds: Investigate the current method of transferring the funds for research money, and create a WWW application that could simplify the process, to include the electronic transfer of funds.

D. THE FUTURE

The future for FTM on the WWW lies not with third party transaction systems, as detailed in this thesis, but with direct Internet access to the credit suppliers. Both Visa and Master Card, the two largest credit card companies, have joined forces to develop an open protocol for the use of any credit card on the Internet. (Visa/Master Card, 1995)

This open protocol would allow the users to purchase goods or services, with funds being exchanged at the credit card company, vice the third party. Although a working protocol may take anywhere from six months to three years to develop and mature, once it does get released to the general WWW population, it is sure to gobble most of the financial market share. In the meantime, systems such as First Virtual and Netbill will continue to provide the necessary tools for the continued growth of Internet commerce. (Visa/Master Card, 1996)

APPENDIX. WORLD WIDE WEB RESOURCES

Because of the fluid nature of the Web, some WWW resources may not be available for review. I have placed those web pages that were most likely to be removed in this appendix.

[redacted] --

First Bank of Internet (FBOI) Opens

Vinn Beigh <fboi@netcom.com >
Sun, 19 Mar 1995 23:03:43 -0800

```
 ___/\___
_|_()_|_                 A N N O U C E M E N T

For immediate release:                 Contact: fboi@netcom.com
Monday, March 20, 1995                 Subject of 'info' for details
                                       Direct questions to Vinn K. Beigh
```

The First Bank of Internet, FBOI, is announcing the initiation of transaction processing services for Internet electronic commerce. Purchases over the Internet can now be made without exposing personal credit card information. Vendors can now sell products on the Internet without the restrictions imposed by credit card use.

Other Internet purchase procedures require personal credit card information. Those proceedings will be monitored by thousands of people all over the world. Some will attempt to either decode the credit card information or impersonate the customer in future transactions.

The alternative to personal credit cards for electronic commerce is based on an FBOI procured Visa (tm) Automated Teller Machine (ATM) card. The card is prepaid, PIN protected, replaceable, disposable, and good at over 200,000 Visa/PLUS (tm) ATMs in 83 countries.

The safety of FBOI is ensured because access to ATM funds without possession of both the ATM card and the Personal Identification Number (PIN) is not possible. ATM cards are also better than credit cards because their purchase does not require the personal, financial, and employment background of the consumer.

The Visa ATM card is not a credit card. It is cash. The ATM card will be used as a checking account. Using an ATM card allows consumers to set aside dedicated funds for Internet data purchases. It provides a safe, secure way to transfer cash from consumers to producers. In addition, consumers can reclaim their funds at any time using an ATM.

A check/invoice procedure is used that consumers will find familiar. The consumer first places an order with a vendor. The consumer then sends to the vendor or FBOI an e-mail 'check' for the purchase of the program/file/data product. The vendor sends FBOI an e-mail 'invoice'. FBOI will reconcile the transaction and send e-mail transaction receipts to both the vendor and customer. Cash will be taken from the customer ATM account and credited to the vendor for later payment. FBOI charges a 5% vendor commission per transaction.

Producers of software, information collections, newsletters, graphics, and other data products can use FBOI services for the sale of their products. These vendors can sell their products for prices that would be too low for credit card transactions. Subscription services that charge an up-front fee for one time access to data depositories and services also can participate.

Vendors will benefit from a very large consumer base because this global solution works just as well outside the U.S. as within the U.S.. The Visa ATM network is worldwide. Consumers will benefit from a very large vendor base because software produced in non-North American countries can be offered for sale much easier than now.

The worldwide producers on the Internet can use FBOI services without the expense of owning or renting a dedicated Internet server or a World-Wide Web site. E-mail is the cheapest and simplest of all Internet services. Large Internet commercial services will soon be starting that provide only for the on-line purchase of catalog products. It will not be possible for the individual producer to sell a data product using those services. Those services will collect the consumers credit card information in advance because of Internet security problems.

FBOI transmits no sensitive information over the Internet and prevents forgery and impersonation by using Pretty Good Privacy, PGP (tm), software for all transactions. This freeware provides excellent authentication and anti-alteration security.

In addition to the unsecured nature of the Internet, consumers should be hesitant giving out their credit card information to vendors of unknown credibility. Tracking is much harder on the Internet than magazine direct marketing. Also, it is not the same as mail order merchandise since U.S. Postal Service and Federal Trade Commission mail order laws do not apply to the Internet.

For high volume, low cost, transactions directly between producers and consumers on the Internet contact FBOI.

Further information can be obtained from The First Bank of Internet by sending an e-mail message with the subject "info" to <fboi@netcom.com>.

Visa is a trademark of Visa International Service Association. PLUS is a trademark of Plus System, Inc. PGP and Pretty Good Privacy are trademarks of Philip Zimmermann. The First Bank of Internet (tm) is not a lending institution, and is not chartered.

Electronic Payment over Open Networks

P. Janson, M. Waidner
IBM Zurich Research Laboratory
CH 8803 Rüschlikon, Switzerland
{pj,wmi}@zurich.ibm.com

April 18th, 1995

A slightly modified version appeared in:
SI INFORMATIK / INFORMATIQUE 3/1995, pp. 10-15

Table of Contents

Abstract: *As business is moving from face-to-face trading, mail order and phone order to electronic commerce over open networks such as the Internet, crucial security issues are being raised. While EFT over financial networks is reasonably secure, securing payments over open networks connecting commercial servers and consumer workstations poses challenges of a new dimension. This paper reviews the state of the art in payment models and technologies, and sketches emerging developments.*

---

1 Introduction

Since the dawn of history there was trading between two parties exchanging goods face-to-face.

Eventually such trading became complicated and money was invented so a buyer could acquire something he needed from a seller without necessarily exchanging goods. Security of the monetary systems was guaranteed by the local, regional, national and eventually international banks controlling the printing of money. New steps were taken when payment orders, cheques, and later `plastic' money were invented. This allowed payment without `actual' money, the mapping between the payment instrument and the real money being still guaranteed by the banks through secure financial clearing networks. Eventually remote payment became possible using those same instruments, although security then started to become a challenge. Indeed verifying a signature on a cheque or a credit card mail order when buyer and seller are not face-to-face is impossible: either the buyer must take the risk of sending in a payment before having received his purchase or the seller must send the purchased items before having received the payment. Phone order purchases are even worse since no signature at all can be provided: the seller runs the risk that the buyer may deny having made the purchase and demand a refund even after he has received the goods. Without new security measures, envisioning electronic commerce over open computer networks is utopic. This paper discusses electronic payment models in Section 2, security requirements in Section 3, and emerging technologies in Section 4.

---

2 Electronic Payment Models

Figure 1: Basic components of a payment system. In principle, all transactions could be performed via the open network, but for security and historical reasons, the existing financial networks will be used for clearing.

Commerce involves always a **buyer** and a **seller** who need to exchange money for goods or services, and at least one financial institution which links "bits" to "money." In most existing payment systems, this role is divided into two parts, an **issuer** (used by the buyer) and an **acquirer** (used by the seller).

The electronic payment from buyer to seller is implemented by a flow of real money from

- buyer to issuer (*withdrawal*, e.g., by buying a phone card using cash, or by moving money out of a debit account, or into a credit account),
- issuer to acquirer (*clearing*),
- acquirer to seller (*deposit*, e.g.,by putting money into the seller's account).

In *pre-paid (debit) payment systems,* the bank account or real purse (if loading cash via a reverse ATM is possible) of the buyer is debited a certain amount which can be used for payments afterwards. Card-based electronic purses, electronic cash as well as (certified/guaranteed) bank cheques fall in this category. In *pay-now payment systems*, the buyer's account is debited at the time of payment. ATM-card based systems (like the European edc-system) fall in this category. In *pay-later (credit) payment*

systems, the seller's bank account is credited the amount of the sale before the buyer's account is debited. Credit card systems fall in this category.

3 Security Requirements

The security requirements of electronic payment systems vary depending on their features and the trust assumptions put on their operation. Therefore, it is not possible to provide a single specification how to secure them. Generally, though, one or more of the following illustrative requirements must be met:

Integrity and authentication:

- ☐ Messages that authorize debit of a buyer's account need to be *signed* by that buyer to guarantee that unauthorized parties, including the issuer itself, cannot draw on the buyer's account without an explicit proof that the buyer authorized the debit.
- ☐ Both the buyer and the banks involved want to make sure that such signed payment authorizations are unique and cannot be submitted twice by a claimed seller.
- ☐ The buyer may demand from the seller a signed acknowledgement that the purchased goods or services were or will be delivered (on-line or off-line depending on the kind of merchandise purchased).
- ☐ Buyer and seller may in fact want a trusted third party to insure fair exchange of the payment for the above signed acknowledgement.
- ☐ The seller may want from the acquirer a guarantee of payment before any goods or services are actually provided to the buyer.

Confidentiality:

- ☐ Some or all parties involved may wish confidentiality of the transaction, whereby identity of the buyer, seller, purchase content, amount, etc., are known only to the participants involved, or even only to a subset of them (e.g., where untraceability is desired).

Availability and Reliability:

- ☐ All parties are interested in being able to perform payments whenever necessary.
- ☐ Payment transactions must be atomic, i.e., happen entirely or not at all, but never hang in an unknown or inconsistent state. No buyer would accept to lose money due to a network crash, or because the seller's server crashed.

Availability and reliability presuppose that the underying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronisation protocols. These fault tolerance issues are not discussed in the following, since most payment systems do not address them explicitly.

To address the security requirements, digital signatures and secret key distribution functions are required, which makes it desirable that all parties involved have access to secure key storage. If payments are to be possible from any workstation, the secret key storage of a user must even be mobile, which in turn makes it necessary that users be provided with smart cards or similar secure devices. These technology options are discussed in the following Section 4, together with some examples.

4 Technology Overview

The main design decision for electronic payment systems is how to authorise payments, i.e., how to enable the honest buyer to convince the seller to accept a legitimate payment while preventing the dishonest buyer from doing unauthorised payments. For instance, it must not be possible to spend the same money twice by sending the same messages to two different sellers. And all this must be done in a way that does not harm the privacy of honest buyers and sellers.

This short of technology overview is structured according to the different techniques used to solve this problem. Thereby, we split the problem into two sub-problems:

- The buyer is *authenticated* as a "legal" payer (e.g., by means of a public-key certificate), and the seller or acquirer are convinced by some protocol that *if* the buyer is honest, *then* the seller will receive the money.
- The payment is *authorised*, i.e., the seller is convinced that he will receive the money.

4.1 On-line vs. off-line

Payments can be performed *on-line*, involving an authentication and authorisation server (usually as part of the acquirer) in each payment, or *off-line*, i.e., without contacting a third party during the payment from buyer to seller.

On-line systems require, of course, more communication, but not necessarily specific tamper-resistant hardware at the buyer and seller. In general, they are considered as more secure than off-line systems. Most proposed *Internet* payment systems are on-line systems.

Off-line *authorisation* systems are more communication efficient, but usually require tamper resistant hardware at the buyer (e.g., smartcards) and sometimes also at the seller (e.g., security modules of POS-terminals).

All proposed *electronic purses* follow this concept, e.g., *Danmont, Proton* (by *Banksys*), *Mondex (1), Express* (by *Europay*), CAFE (2) (developed by a European ESPRIT consortium). The "exotic" systems in this list are *Mondex* and *CAFE. Mondex* is the only system that enables off-line transferability (i.e., the seller can use the amount received for a new payment, without intermediate deposit --- but this seems to be a politically unpopular feature in most countries) and is considered for high-value payments

(i.e., beyond 100 ECU). *CAFE* is the only system that provides strong buyer anonymity and untraceability. Both systems offer the buyers an *electronic wallet*, preventing the well-known fake-terminal attacks on the buyer's PIN. *Mondex, Express,* and *CAFE* are multi-currency purses, i.e., they can handle different currencies simultaneously.

All these systems could be used for Internet payments, but currently, they aren't. The main obstacle is that they require a smartcard reader attached to the buyer's PC or workstation. Inexpensive PCMCIA smartcard readers and standardised infrared-interfaces on notebook computers can solve this connectivity problem. This is the approach taken in the recently announced First Bank of Internet system, based on the newly announced VISA electronic purse.

Another system that will be developed in this spirit is the *FSTC Electronic Check*, that will use a tamper-resistant PCMCIA card, and will implement a cheque-like payment model.

Alternatively to tamper-resistant hardware, off-line authorisation could be done via *pre-authorisation*, i.e., the seller is known in advance, and the payment is already authorised during withdrawal, in a way similar to a certified bank cheque.

Whether off-line *authentication* requires tamper-resistant hardware or not, depends on the cryptographic primitives used, and on how trustworthy the buyer's PC or workstation is from the buyer's point of view.

4.2 Tamper-resistant Hardware

As already mentioned in Section 4.1, for the issuer's security, most off-line payment systems require a piece of tamper-resistant hardware in the buyer's device. In a certain sense, this piece is a "pocket branch" of the issuer.

Independent of the issuer's security considerations, it might also be in the buyer's interest to have a secure device, protecting the buyer's secret keys. Initially, this could be just a smartcard, but in the long run, it should be at least a smartcard reader with its own keyboard and display for entering a PIN and simple commands. This is often called an *electronic wallet.*

Without such a secure device, the buyer's secrets, i.e., the buyer's money, are vulnerable to anybody who can access the buyer's machine. This is obviously a problem in multi-user environments, but also on single-user machines that may be accessed directly or indirectly by others, and where a virus, for instance, could steal PINs and passwords while they are entered.

Even with a smartcard, the buyer cannot be sure that a Trojan horse in his or her PC cannot reveal PINs of credit cards by sending mail to a remote attacker, or by simply asking the smartcard to make a payment to the attacker's account, silently. Therefore, for real security trusted input and output channels between user and "pocket workstation" must exist, e.g., using an electronic wallet with its own display and keypad.

4.3 Cryptography

"Crypto-less" Systems

Using *no cryptography* at all means relying on "out-band" security: For instance, the goods ordered electronically are not delivered before a fax (or a letter, or a phone call) arrives from the buyer that acknowledges this order.

Examples for this kind of systems are *CompuServe*, *First Virtual*, and the *Internet Shopping Network*. In *CompuServe*, each customer uses a line to dial into the system that is assumed to be secure by itself, and identifies himself or herself to the system. For both *First Virtual* and the *Internet Shopping Network*, the buyer has an account with the system and receives a password in exchange for a credit card number. The password is not protected while travelling over the *Internet*, i.e., these systems are vulnerable against eavesdropping. *First Virtual* has some protection by asking the supposed buyer for an acknowledgment of each payment via email, but the actual security of the system is based on the fact that buyers can revoke *each* payment within a certain time (i.e., there is no definite authorisation during the payment).

Generic "Payment Switch"

A special role is played by the *OpenMarket Payment Switch* (3): It is an on-line payment system implementing both, a pre-paid and pay-later models. It supports *several* authentication methods, depending on the payment method chosen, ranging from simple, unprotected PIN-based authentication to challenge-response based systems, where the response is computed, e.g., by a smartcard.

Actually, *OpenMarket* uses passwords and optionally two types of devices for response generation, *Secure Net Key* and *SecureID*, i.e., shared-key cryptography. (For authorisation, the *Payment Switch* digitally signs an authorisation message sent to the seller, i.e., public-key cryptography is used for this special purpose.)

Shared-key Cryptography

For *shared-key cryptography*, the buyer and merchant on the one side and that party performing authentication or authorisation on the other side need a shared secret (e.g., a DES-key (4), or at least a password/PIN).

Since both sides have exactly the same information, this cannot provide *non-repudiation* (e.g., if buyer and issuer disagree about a certain payment, there is no way to decide whether this payment was initiated by the buyer, or by a dishonest employee of the issuer), and is therefore not recommended for high-value payments (say, greater than 100 ECU).(5)

If authentication should be done off-line (which is desirable at least for low-value payments), each pair of buyer and merchant need a shared secret key. In practice this means that some sort of master-key is present at each merchant, enabling the merchant to derive the buyer's key, e.g., from the buyer's identity. Usually, tamper-resistant security modules in point-of-sale terminals are used to protect this key. (6)

Shared-key cryptography is used, e.g., by the off-line systems *Danmont* and *Proton,* and the on-line systems SNPP (7), NetBill (8) (by *Carnegie Mellon University, CMU*), and NetCheque (9) (by *University of Southern California*).

NetBill and *NetCheque* are based on the Kerberos technology, and focus on "micro-payments." Both implement a cheque-like debit payment model. The use of shared-key technology is justified by the performance required to process many micro-payments in short time.

In February 1995, *VISA* and *CMU* announced a cooperation to develop *NetBill*, probably in the direction of using asymmetric cryptography, for commercial purposes.

Public-key Cryptography

For public-key cryptography, the buyer has a secret signature key and a certificate for his corresponding public signature verification key (e.g., issued by the payment system operator or a specific issuer). In most existing and proposed systems, RSA is used (but there are several alternatives).

Digital signatures provide *non-repudiation*, i.e., disputes between sender and recipient of a signed message can be resolved. This should be mandatory at least for high-value payments.

Off-line *authentication* is no problem here, since the seller can easily verify a signature of the buyer (and could check the certificate against a local copy of a blacklist of "bad" certificates, if necessary). Authorisation still requires either an on-line connection or trusted hardware at the buyer.

Public-key cryptography will be used, e.g., by the off-line systems *Express* (by *Europay*) and *CAFE*. Most of the proposed on-line payment systems use public key cryptography:

Rather *general WWW security schemes* using public-key cryptography are SHTTP and SSL. Neither is a payment technology per se, but they are suggested for securing also payment information.

SSL is an Internet socket-layer communication interface allowing buyer and seller to communicate securely. Netscape Communications Corporation (which proposed SSL) is offering payment mechanisms based on that secure interface. SSL does not support non-repudiation.

SHTTP is a secure extension of the HTTP protocol used on the Internet World-Wide Web (WWW), developed by the CommerceNet consortium. SHTTP offers several security techniques, e.g., signing and encrypting with RSA, on top of which various payment protocols may and will be implemented.

Both SSL and SHTTP offer a selection of symmetric and asymmetric cryptographic technologies. Because of the open access these technologies offer to strong cryptographic primitives, they are all subject to U.S. export restrictions. Exportable versions will be available but they will be using `tamed' (less secure) cryptographic technologies. It is very questionable whether banks, merchants, and customers outside North America will be interested in such `second-grade' technologies.

Complete payment systems using public-key cryptography are, e.g., ecash (by *DigiCash*), NetCash (by *University of Southern California*), Cybercash, and *iKP* (10) (by *IBM*).

In November 1994 *VISA* and *Microsoft* announced a common plan to develop and offer secure payment technology based on *RSA* technology, but not much more is publicly known about the design as of this writing.

IBM is developing an open payment technology, *iKP*, implementing a credit-card-like payment model that easily connects to the existing credit card clearing networks. The payment logic is bundled with strong cryptographic mechanisms that are not accessible to other applications. The objective is that such a design should be exportable according to the U.S. law and importable to almost any other country, thus forming a valuable basis for an internationally usable open and secure technology. Furthermore, the technology is designed so that it can operate transparently with any WWW browser and server on any platform, unlike some other designs that require specially equipped browsers and servers.

4.4 Anonymity of Buyer

Some payment systems provide buyer anonymity and untraceability. Both are considered useful for cash-like payments (say, up to 100 ECU), with the argument that real cash is also anonymous and untraceable, and that buyers do not want to enable a third party to trace all their everyday-payments, certainly not the sellers (shops, publishers, etc.), but in some cases not even the banks.

While *anonymity* simply means that the buyer's identity is not used in payments, *untraceability* means that the buyer cannot be identified, and even that two different payments of the same buyer cannot be linked. Both properties hold with respect to the seller only or with respect to both seller and issuer/acquirer.

All payment systems could made untraceable by *outsiders,* by encrypting all flows between buyer and seller, and anonymous to seller by using pseudonyms instead of real identities.

Some electronic payment systems are designed in a way which provides anonymity or even untraceability with respect to the seller (e.g., *iKP* (10) offers this as one option).

Currently the only payment systems mentioned here that provide anonymity and untraceability against seller *and* issuer/acquirer are ecash (on-line) and *CAFE* (1) (off-line, based on smartcards), both based on asymmetric cryptography (a special form of signatures called *blind signatures* (11)).

NetCash and *ACC* (12) also provide anonymity and untraceability, but based on the use of trusted "mixes" that change electronic money of one representation into another representation, without revealing the relation. Neither ecash nor CAFE assume the existence of such trusted third parties.

5 Summary and Outlook

Because of the limited space in this article, we were not able to describe the technical details of the different payment systems listed. However, even the high-level overview and the rich set of references should have made it clear that the *technology* that is necessary for secure electronic *Internet* payment systems already exists. Achieving security for all parties, inclusive perfect untraceability for the buyer, is possible.

Currently, no proposal or system is dominant, but with high probability this will change within the next two years at most. But the question "Which payment system will be used on the *Internet*?" will not have a single answer. Several payment systems will coexist:

- Micro-payments (less than 1 ECU), low-value payments (1-100 ECU) and high-value payments have significantly different security and cost requirements.

Possibly, high values will be transferred using non-anonymous, on-line payment systems based on asymmetric cryptography, implementing a cheque-like or credit-card-like payment model. As soon as smartcard readers are available at PCs and workstations, small amounts might be paid using pre-paid off-line payment systems that provide a certain degree of untraceability (like real cash).

- Payment systems with and without tamper-resistant hardware at the buyer will coexist for some time. Ultimately, payment systems based on smartcards and electronic wallets (having their own display and keyboard, and communicating with the buyer's terminal via an infrared interface) will become dominant, since they clearly provide better security and enable the buyer to use untrusted terminals without endangering security.
- Probably, a few almost equivalent payment systems will coexist for the same areas of application (i.e., payment model and maximum amounts). The reasons are various "cultural" differences in the business and payment processes (e.g., between the U.S. and Europe), national security considerations that might disable some solutions in some countries, and competition between payment system providers.

Footnotes

(1) http://www.mondex.com/mondex/home.htm; see also: Richard Rolfe: Here Comes Electronic Cash; Credit Card Management Europe, January/February 1994, 16-20.

(2) http://www.zurich.ibm.ch/Technology/Security/sirene/projects/cafe/index.html; see also Jean-Paul Boly et.al.: The ESPRIT Project CAFE - High Security Digital Payment Systems; ESORICS '94, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

(3) http://www.openmarket.com/about/technical/; see also: David K. Gifford, Lawrence C. Stewart, Andrew C. Payne, G. Winfield Treese: Payment Switches for Open Networks; IEEE COMPCON, March 95.

(4) We do not provide references to cryptographic algorithms in this overview. For an introduction and a description of most of the cryptographic algorithms used for electronic payment systems,

see Bruce Schneier: Applied Cryptography; John Wiley & Sons, 1994.
(5) For some examples on the consequences of no non-repudiation see: Ross Anderson: Why Cryptosystems Fails; Communications of the ACM 37 11, November 1994, 32-41.
(6) For an example, see: Integrated Circuit Card Specifications for Payment Systems; Europay/MasterCard/VISA, October 1994.
(7) Semyon Dukach: SNPP: A Simple Network Payment Protocol; Computer Security Applications Conference, 1992.
(8) http://www.ini.cmu.edu/netbill; see also: Marvin Sirbu, J. D. Tygar: NetBill: An Internet Commerce System; IEEE COMPCON, March 95.
(9) Clifford Neuman, Gennady Medvinsky: Requirements for Network Payment: The NetCheque Perspective; IEEE COMPCON, March 95.
(10) http://www.zurich.ibm.ch/Technology/Security/extern/ecommerce/; see also: Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner: iKP A Family of Secure Electronic Payment Protocols; IBM T.J. Watson Research Centre and IBM Zürich Research Lab, Draft, March 1995.
(11) David Chaum: Achieving Electronic Privacy; Scientific American, August 1992, 96-101. David Chaum: Privacy Protected Payments; SMARTCARD 2000, North-Holland, Amsterdam 1989, 69-93.
(12) http://www.research.att.com/index.html#acc; see also: Steven H. Low, Nicholas F. Maxemchuk, Sanjoy Paul: Anonymous Credit Cards; 2nd ACM Conference on Computer and Communication Security, Fairfax 1994.

Last modified: Thursday, 24-Aug-95 14:25:37 CUT

For Immediate Release

Visa and MasterCard Working Together to Support Specifications for Secure Card Transactions on the Internet

Transactions on the Internet

NEW YORK & SAN FRANCISCO, June 23, 1995 -- MasterCard International and Visa International today announced that the two associations will integrate their current efforts to provide a method for secure bankcard purchases on open networks such as the Internet. Consumers around the world hold more than 690 million bankcards, and with this security it means using those cards to conduct transactions in cyberspace will soon be as secure as using a card at a physical point of sale today.

Visa and MasterCard will support specifications expected to be published by September, and anticipate that consumers will begin participating in secure card transactions on the Internet in early 1996. As a first step, the associations are agreeing upon a common set of requirements and sharing technical information.

The security specification supported by MasterCard and Visa will be open and available to all entities. This standard will provide payment security for all bankcard transactions; other security protocols can be used to protect personal data. The new standard also will facilitate deployment of personal-computer (PC) software to incorporate payment-security applications.

"The first requirement necessary to grow a new market is consumer and merchant confidence. A secure transaction within a secure payment system is the foundation of that confidence," said Edmund Jensen, president and CEO of Visa International. "Establishing that environment for our member financial institutions -- and their consumers and merchants -- is the purpose of our groundbreaking efforts to forge partnerships that bridge the worlds of high-tech and financial services. Working together to build a common security payment standard for bankcard acceptance and use is a crucial step in the development of electronic commerce -- and will be the significant enabler in the commercial growth of the Internet."

"Establishing one standard for card purchases on the Internet is absolutely the right thing to do for consumers, merchants and financial institutions worldwide," said H. Eugene Lockhart, CEO of MasterCard. "The industry has a rich history of setting standards --the global chip-card specifications are an excellent example -- that benefit consumers worldwide. And, it's exciting that we will do the same in

The card associations will separately test SET with consumers, merchants and financial institutions. A joint interoperability test will be conducted after the individual tests to ensure SET, where necessary, operates as smoothly as the point-of-sale system used today. Upon conclusion of the tests, an updated version of the specification will be published for software providers.

MasterCard's Web address is http://www.mastercard.com. Visa's Web address is http://www.visa.com.

MasterCard International Incorporated is a global payments company that provides consumer credit, debit and other payment products in partnership with 22,000 member financial institutions worldwide. MasterCard's family of brands, MasterCard(R), Maestro(R) and Cirrus(R), represent approximately 300 million cards in circulation, and over 13 million acceptance locations, including 243,000 MasterCard/Cirrus ATMs worldwide. MasterCard's pioneering work in the areas of transaction processing and delivery systems continues to revolutionize the way consumers pay for goods and services.

Headquartered in the San Francisco Bay Area, Visa is the world's largest payment system. It plays a pivotal role in developing and implementing new technologies that benefit its 19,000 member financial institutions and their cardholders, businesses, governments and the global economy. Visa's 442 million cards are accepted by more than 12.2 million merchants worldwide. Visa/PLUS is the largest global ATM network.

###

For Immediate Release

Visa & MasterCard Combine Secure Specifications For Card Transactions On The Internet Into One Standard

Move expected to accelerate development of electronic commerce and bolster consumer confidence in the security of cyberspace transactions

PURCHASE, NY & SAN FRANCISCO, February 1, 1996 -- Addressing consumer concerns about making purchases on the Internet, MasterCard International and Visa International joined together today to announce a technical standard for safeguarding payment-card purchases made over open networks such as the Internet. Prior to this effort, Visa and MasterCard were pursuing separate specifications. The new specification, called Secure Electronic Transactions (SET), represents the successful convergence of those individual efforts. A single standard means that consumers and merchants will be able to conduct bankcard transactions in cyberspace as securely and easily as they do in retail stores today.

The associations expect to publish SET on their World Wide Web sites in mid-February. Following a comment period, the joint specification is scheduled to be ready for testing in the second quarter 1996. Visa and MasterCard expect that banks will be able to offer secure bankcard services via the Internet to their cardholders in the fourth quarter 1996.

Participants in this effort with MasterCard and Visa are: GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems and Verisign. Also, SET will be based on specially developed encryption technology from RSA Data Security.

"This is the first step in making cyberspace a profitable venture for banks and merchants. A single standard limits unnecessary costs and builds the business case for doing business on the Internet," said Edmund Jensen, president and CEO of Visa International. "Further, our work with MasterCard demonstrates our unwavering commitment to address the needs of our member financial institutions, and their merchants and cardholders."

H. Eugene Lockhart, CEO of MasterCard, said: "MasterCard has viewed one open standard for secure card purchases on the Internet as a critical catalyst for electronic commerce because it bolsters consumer confidence in the security of the electronic marketplace. A single standard has always been our objective because it is in the best interests of not only consumers, but also merchants and financial institutions worldwide. We are glad to work with Visa and all of the technology partners to craft SET."

the dynamic environment of the Internet. Our objective is to ensure that every transaction, no matter what type it is and no matter where it occurs, is processed quickly, securely and reliably."

The specifications supported by the associations will call for the use of extensive encryption capabilities based on RSA Data Security to protect card transactions on the Internet and other networks. And, MasterCard and Visa anticipate that purchases and payments performed on open networks such as the Internet will function similarly to other bankcard purchases.

Protecting card transactions over open networks is crucial for both card associations. Bankcards represent the best payment option for users of the Internet, and that use will expand exponentially as the market continues its explosive growth. Protecting and leveraging their powerful brands in a non-physical world will be key to Visa and MasterCard. With a combined global-transaction volume of more than $1 trillion, the associations' joint work in establishing security standards on the Internet will be a forceful engine for its continued growth.

###

LIST OF REFERENCES

(Bhargava, 1996) - Bhargava, H.K., Krishnan, R., Muller, R., "Decision support on Demand: Emerging Electronic Markets for Decision Technologies," 22 February 1996,

(Brands, 1995) - Brands, S., "Electronic Cash on the Internet," pp. 64-84, *IEEE Publications*, April 1995.

(Carter, 1995) - Carter, D., "Computer Crimes Greater Than Expected, Increasing," *Newsbytes*, 25 October, 1995.

(Cox, 1994) - Cox, B.T.H., *Maintaining Privacy in Electronic Transactions*, Carnegie Mellon University, August 1994.

(Deephouse, 1995) - Deephouse, C. Netbill Project Team, E-mail interview conducted 9 October, 1995.

(Deephouse, 1995) - Deephouse, C. Netbill Project Team, E-mail interview conducted 13 February, 1996.

(Dukach, 1992) - Dukach, S., "SNNP: A Simple Network Payment Protocol,", pp. 173-179 *Proceedings of Computer Security Applications Conference*, November, 1992.

(First Bank, 1994) - "First Bank of the Internet, Announcement of Business", http://catless.ncl.uc.uk/Risks/16.93.html#subj:11, 1995.

(FV Background, 1995) - "First Virtual Frequently Asked Questions: Background," http://www.fv.com:80/FAQ/index.html, 1995.

(FV Buying, 1995) - "First Virtual Frequently Asked Questions: Buying," http://www.fv.com:80/FAQ/index.html, 1995.

(FV Cashflow, 1995) - "First Virtual Frequently Asked Questions: Cashflow," http://www.fv.com:80/FAQ/index.html, 1995.

(FV General, 1995) - "First Virtual Frequently Asked Questions: General Information," http://www.fv.com:80/FAQ/index.html, 1995.

(FV Infohaus, 1995) - "First Virtual Frequently Asked Questions: Infohaus," http://www.fv.com:80/FAQ/index.html, 1995.

(FV Security, 1995) - "First Virtual Frequently Asked Questions: Security,"

http://www.fv.com:80/FAQ/index.html, 1995.

(FV Selling, 1995) - "First Virtual Frequently Asked Questions: Selling," http://www.fv.com:80/FAQ/index.html, 1995.

(Fitzgerald, 1993) - Fitzgerald, J., *Business Data communications: Basic Concepts, Security and Design*, John Wiley & Sons, New York, New York, 1993.

(Gelormine, 1995) - Gelormine, V., "Selling in Cyberspace," *Selling Success*, May 1995.

(IETF, 1995) - Internet Engineering Task Force Home Page, http://www.ietf.cnri.reston.va.us/home.html.

(IRS, 1996) - Internal Revenue Service, "Tax Supplement - Business Information," http://www.irs.ustreas.gov/plain/news/supplement/96taxsup.bus.html, January 1996.

(Janson, 1995) - Janson, P., Waidner, M., "Electronic Payment over Open Networks," http://www.zurich.ibm.ch/Technology/security/extern/ecommerce/, April, 1995.

(Lessa, 1995) - Lessa, K.D., J.C. Penny Unix Systems Project Manager, E-mail interview conducted August, 1995.

(Little, 1994) - Little, T.,"Commerce on the Internet,"p. 74, *IEEE Winter*, 1994.

(Medvinsky, 1993) - Medvinsky, G., Newmann, B., "Netcash: A Design for Practical Electronic Currency on the Internet," *Proceedings of the First ACM Conference on computers and communications Security*, November, 1993.

(Netbill, 1994) - Netbill Home Page, http://www.ini.cmu.edu/NETBILL/, 1995.

(Polsson, 1995) - Polsson, K. "Chronology of the Events in the History of Microcomputers," http://www.islandnet.com/~kplosson/comphist.htm, 1995.

(Tardif, 1995) - Tardif V., "Sniffers and Spoofers," *Internet World*, Vol 6 No 12, December, 1995.

(Siino, 1994) - Siino, R., "First Data Brings Secure Payment Processing to the Internet With Mosaic Communications Software," Mosaic Communications Corp Press Release, November 1994.

(Sirbu, 1995) - Sirbu, M., Tygar, D., "Netbill: An Internet Commerce System Optimized for Network Delivered Services," http://www.ini.cmu.edu/NETBILL/ publications/CompCon_TOC.html , 1995.

(Spyglass, 1994) - Spyglass, Inc., "Electronic Commerce Standards for the WWW," Spyglass White Paper, Savoy, Illinois, December 1994.

(Stein, 1994) - Stein L., Steferud, E., Borentstein, N., Rose, M., *The Green Commerce Model*, October, 1994.

(Vacca, 1995) - Vacca J., "Mosaic: Beyond Net Surfing," p. 75, *BYTE*, Vol 20, No 1, Peterborough, NH, January, 1995.

(Visa/Master Card, 1995) - "Visa And Master Card Working Together to Support Specifications for Secure Card Transactions on the Internet," http://www.Mastercard.com/Press/release-950623.htm, 1995.

(Visa/Master Card, 1996) - "Visa & MasterCard Combine Secure Specifications For Card Transactions On The Internet Into One Standard," http://www.Mastercard.com/Press/release-960201.htm, 1996.

(Wall Street Journal, 1994) - "Systems Planned for Shopping in the Internet," pp. B1, Wall Street Journal, New York, New York, 13 September, 1994.

(W3C, 1995) - World Wide Web Consortium Home Page, http://www.w3.org/htpertext/www/Consortium/, 1995.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Professor Hemant K. Bhargava 4
   Department of Systems Management (Code SM/Bh)
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Gordon Bradley 1
   Department of Operational Research (Code OR/Bz)
   Naval Postgraduate School
   Monterey, CA 93943

5. Professor Ted Lewis 1
   Department of Computer Science (Code CM/Lt)
   Naval Postgraduate School
   Monterey, CA 93943

6. Professor Rex Buddenberg 1
   Department of Systems Management (Code SM/Bu)
   Naval Postgraduate School
   Monterey, CA 93943

7. Art Geoffrion 1
   Graduate School of Management
   UCLA
   405 Hilgard Ave.
   Los Angeles, CA 90024-1481

8. Professor Steven O. Kimbrough 1
   The Wharton School
   Operations & Information Management Dept.
   3620 Locust Walk
   Philadelphia, PA 19104-6366

9. Professor Ramayya Krishnan..1
The Heinz School
Carnegie Mellon University
Pittsburgh, PA 15213

10. Professor Rudolf Muller...1
Institute for Information Systems
Humboldt\University Berlin
Spandauer Str. 1, 10178
Berlin, Germany

11. Dr. Michael J. Mesgtrovich...1
Deputy Director, Joint Requirements Analysis and Integration (D-7)
Defense Information Systems Agency
5201 Leesburg Pike, Suite 1501
Falls Church, VA 22401